T S5/5/1

5/5/1
DIALOG(R)File 351:Derwent WPI
(c) 2005 Thomson Derwent. All rts. reserv.

013608276
WPI Acc No: 2001-092484/200111
XRPX Acc No: N01-069981
Electronic storage device for guaranteeing originality of electronic data varies level of access based on if data are original data or not
Patent Assignee: RICOH KK (RICO)
Inventor: KANAI Y; YACHIDA M
Number of Countries: 002 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 10024753	A1	20001221	DE 1024753	A	20000519	200111	B
JP 2000339223	A	20001208	JP 99145340	A	19990525	200113	
JP 2001005728	A	20010112	JP 99173371	A	19990618	200118	
JP 2001147898	A	20010529	JP 99328802	A	19991118	200136	
JP 2001154577	A	20010608	JP 99338741	A	19991129	200138	
JP 2001209582	A	20010803	JP 200015092	A	20000124	200150	
JP 2001209581	A	20010803	JP 200015091	A	20000124	200150	

Priority Applications (No Type Date): JP 200015092 A 20000124; JP 99145340 A 19990525; JP 99173371 A 19990618; JP 99328802 A 19991118; JP 99338741 A 19991129; JP 200015091 A 20000124
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 10024753	A1		159	G06F-012/14	
JP 2000339223	A		29	G06F-012/14	
JP 2001005728	A		46	G06F-012/14	
JP 2001147898	A		11	G06F-015/00	
JP 2001154577	A		12	G09C-001/00	
JP 2001209582	A		18	G06F-012/14	
JP 2001209581	A		16	G06F-012/14	

Abstract (Basic): DE 10024753 A1

NOVELTY - The storage device includes a storage unit which stores electronic data consisting of a number of content files as a single original in an identifiable state. An access unit controls the access to the original electronic data at a level which is different from the level of access to non-original electronic data. The storage unit stores tamper detection information as original information corresponding to the electronic data.

DETAILED DESCRIPTION - The storage device may include a tamper detection information computing device which receives a request to re-store the electronic data as a single original using an encryption key to compute tamper detection information for each of the content files. A second tamper detection information computing device uses the encryption key to compute second temper detection information for edition management information. INDEPENDENT CLAIMS are included for an electronic storage device, an authorization verification system, an electronic storage method, an authorization verification method, damage recovery method and a storage medium for storing a program in a computer.

USE - For originality-guarantee electronic preservation systems using large-capacity storage media.

ADVANTAGE - Allows the originality of a combined document comprising multiple files to be guaranteed.

```
        pp; 159 DwgNo 0/74
Title Terms: ELECTRONIC; STORAGE; DEVICE; GUARANTEE; ELECTRONIC; DATA; VARY
  ; LEVEL; ACCESS; BASED; DATA; ORIGINAL; DATA
Derwent Class: P85; T01
International Patent Class (Main): G06F-012/14; G06F-015/00
International Patent Class (Additional): G06F-003/06; G06F-009/06;
  G06F-012/00; G06F-012/16; G06F-017/30; G06F-017/60; G09C-001/00
File Segment: EPI; EngPI
?
```

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－154577
（P2001－154577A）
(43)公開日　平成13年６月８日(2001.6.8)

(51)Int.Cl.'	識別記号	Ｆ Ｉ		テーマコード'(参考)
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ	５Ｂ０６５
Ｇ０６Ｆ　3/06	３０４	Ｇ０６Ｆ　3/06	３０４Ｈ	５Ｊ１０４
				９Ａ００１

審査請求　未請求　請求項の数７　ＯＬ　（全 12 頁）

(21)出願番号　特願平11－338741

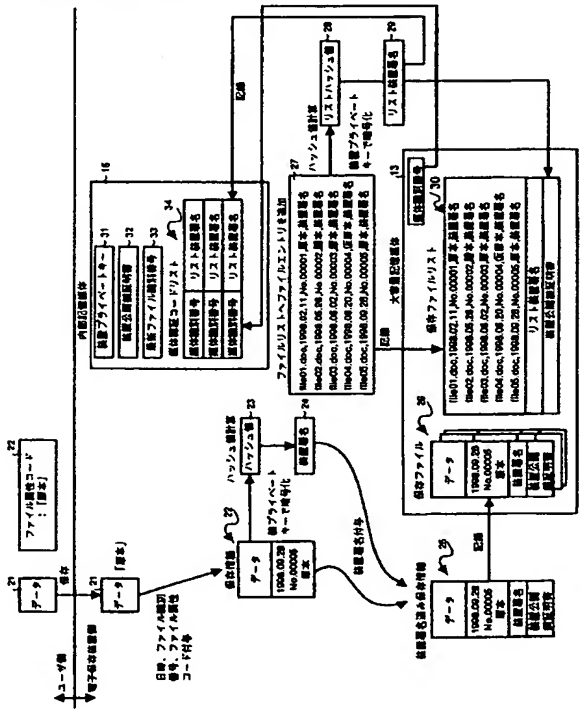
(22)出願日　平成11年11月29日(1999.11.29)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　金井　洋一
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　谷内田　益義
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(74)代理人　100089118
弁理士　酒井　宏明

最終頁に続く

(54)【発明の名称】　原本性保証電子保存装置、原本性保証電子保存方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　大容量記憶媒体の状態を過去の状態に戻すというような大容量記憶媒体の不正なすり替えを効率良く防止すること。
【解決手段】　電子データを保存する際に、媒体識別番号とリスト装置署名２９との対からなる媒体認証コードリスト３４を内部記録媒体１５に記憶しておき、大容量記憶媒体１３を装置本体に装着してマウント処理をおこなう際に、保存ファイルリストの検証処理をおこなって、大容量記憶媒体１３の妥当性を検証する。



1

【特許請求の範囲】

【請求項１】　電子データを記憶する大容量記憶媒体および暗号鍵などを記憶する内部記憶媒体を少なくとも有し、前記電子データの原本性を保証する原本性保証電子保存装置において、

前記大容量記憶媒体に保存するファイルのリストを示すファイルリストを暗号化した署名情報並びに該大容量記憶媒体の媒体識別情報に基づいて前記大容量記憶媒体の正当性を検証することを特徴とする原本性保証電子保存装置。

【請求項２】　前記大容量記憶媒体に保存する保存ファイルのリストを示すファイルリストのハッシュ値を暗号化したリスト署名と、前記大容量記憶媒体の媒体識別情報とを対応づけた媒体認証コードリストを作成する媒体認証コードリスト作成手段と、

前記媒体認証コードリスト作成手段により作成された媒体認証コードリストに基づいて前記大容量記憶媒体の正当性を検証する正当性検証手段と、

を備えたことを特徴とする請求項１に記載の原本性保証電子保存装置。

【請求項３】　前記媒体認証コードリスト作成手段により作成された媒体認証コードリストを前記内部記憶媒体に格納し、前記大容量記憶媒体を装置本体に装着する際に、前記内部記憶媒体に格納された媒体認証コードリストに基づいて前記大容量記憶媒体の正当性を検証することを特徴とする請求項２に記載の原本性保証電子保存装置。

【請求項４】　暗号鍵などを記憶する内部記憶媒体を用いて大容量記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存方法において、

前記大容量記憶媒体に保存するファイルのリストを示すファイルリストを暗号化した署名情報並びに該大容量記憶媒体の媒体識別情報に基づいて前記大容量記憶媒体の正当性を検証することを特徴とする原本性保証電子保存方法。

【請求項５】　前記大容量記憶媒体に保存する保存ファイルのリストを示すファイルリストのハッシュ値を暗号化したリスト署名と、前記大容量記憶媒体の媒体識別情報とを対応づけた媒体認証コードリストを作成する媒体認証コードリスト作成工程と、

前記媒体認証コードリスト作成工程により作成された媒体認証コードリストに基づいて前記大容量記憶媒体の正当性を検証する正当性検証工程と、

を含んだことを特徴とする請求項４に記載の原本性保証電子保存方法。

【請求項６】　前記媒体認証コードリスト作成工程により作成された媒体認証コードリストを前記内部記憶媒体に格納し、前記大容量記憶媒体を装置本体に装着する際に、前記内部記憶媒体に格納された媒体認証コードリストに基づいて前記大容量記憶媒体の正当性を検証することを特徴とする請求項５に記載の原本性保証電子保存方法。

2

【請求項７】　前記請求項３～６のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、電子データを記憶する大容量記憶媒体および暗号鍵などを記憶する内部記憶媒体を少なくとも有し、前記電子データの原本性を保証する原本性保証電子保存装置、原本性保証電子保存方法および記録媒体に関し、特に、大容量記憶媒体の状態を過去の状態に戻すというような大容量記憶媒体の不正なすり替えを効率良く防止することができる原本性保証電子保存装置、原本性保証電子保存方法および記録媒体に関する。

【０００２】

【従来の技術】近年のコンピュータ技術の進展に伴うペーパーレス化の進展に伴って、紙によって原本書類として保存されていた情報が電子データの形式で保存される場合が増えてきたため、かかる電子データの原本性を保証する従来技術が知られている。

【０００３】たとえば、「金井他：原本性保証電子保存システムの開発－システムの構築－，Medical Imaging Tecnology, Vol.16, No.4, Proceedings of JAMIT Annual Meeting'98(1998)」や、「国分他：原本性保証電子保存システムの開発，（特）情報処理振興事業協会発行　創造的ソフトウエア育成事業およびエレクトロニック・コマース推進事業　最終成果発表会論文集　創造的ソフトウエア育成事業編(1998)」には、電子データの原本性を保証するシステムの一例が開示されている。

【０００４】かかる従来技術を用いると、電子データの原本性を保証することが可能となり、これにより原本書類を電子データの形式で保存し、もって高度情報化社会の推進並びに社会全体の生産性向上に寄与することができる。

【０００５】

【発明が解決しようとする課題】しかしながら、これらの従来技術では、各ファイルのデータにメッセージ認証子を付加することでファイルの改ざんを検知しているため、たとえば大容量記憶媒体の状態を過去の状態に戻すというような大容量記憶媒体の不正なすり替えがおこなわれた場合に対応できないという問題がある。

【０００６】特に、たとえば大規模なペーパーレス化を図るような場合には、数多くの大容量記憶媒体を用いねばならず、いきおい第三者がこの大容量記憶媒体に係る不正なすり替えをおこない得るケースが増加し、この大容量記憶媒体に係る不正なすり替えをいかに防止するかが極めて重大な課題となる。

【０００７】この発明は、上記問題（課題）に鑑みてなされたものであり、大容量記憶媒体の状態を過去の状態に戻すというような大容量記憶媒体の不正なすり替えを効率良く防止することができる原本性保証電子保存装置、原本性保証電子保存方法および記録媒体を提供することを目的とする。

【０００８】

【課題を解決するための手段】上記目的を達成するために、請求項１の発明に係る原本性保証電子保存装置は、電子データを記憶する大容量記憶媒体および暗号鍵などを記憶する内部記憶媒体を少なくとも有し、前記電子データの原本性を保証する原本性保証電子保存装置において、前記大容量記憶媒体に保存するファイルのリストを示すファイルリストを暗号化した署名情報並びに該大容量記憶媒体の媒体識別情報に基づいて前記大容量記憶媒体の正当性を検証することを特徴とする。

【０００９】この請求項１の発明によれば、大容量記憶媒体に保存するファイルのリストを示すファイルリストを暗号化した署名情報並びに該大容量記憶媒体の媒体識別情報に基づいて大容量記憶媒体の正当性を検証することとしたので、大容量記憶媒体の状態を過去の状態に戻すというような大容量記憶媒体の不正なすり替えを効率良く防止することができる。

【００１０】また、請求項２の発明に係る原本性保証電子保存装置は、前記大容量記憶媒体に保存する保存ファイルのリストを示すファイルリストのハッシュ値を暗号化したリスト署名と、前記大容量記憶媒体の媒体識別情報とを対応づけた媒体認証コードリストを作成する媒体認証コードリスト作成手段と、前記媒体認証コードリスト作成手段により作成された媒体認証コードリストに基づいて前記大容量記憶媒体の正当性を検証する正当性検証手段と、を備えたことを特徴とする。

【００１１】この請求項２の発明によれば、大容量記憶媒体に保存する保存ファイルのリストを示すファイルリストのハッシュ値を暗号化したリスト署名と、大容量記憶媒体の媒体識別情報とを対応づけた媒体認証コードリストを作成し、作成した媒体認証コードリストに基づいて大容量記憶媒体の正当性を検証することとしたので、この媒体認証コードリストを用いて大容量記憶媒体の正当性を効率良く検証することができる。

【００１２】また、請求項３の発明に係る原本性保証電子保存装置は、前記媒体認証コードリスト作成手段により作成された媒体認証コードリストを前記内部記憶媒体に格納し、前記大容量記憶媒体を装置本体に装着する際に、前記内部記憶媒体に格納された媒体認証コードリストに基づいて前記大容量記憶媒体の正当性を検証することを特徴とする。

【００１３】この請求項３の発明によれば、媒体認証コードリストを前記内部記憶媒体に格納し、大容量記憶媒体を装置本体に装着する際に、この内部記憶媒体に格納された媒体認証コードリストに基づいて大容量記憶媒体の正当性を検証することとしたので、内部記憶媒体を有効に利用して大容量記憶媒体の正当性を効率良く検証することができる。

【００１４】また、請求項４の発明に係る原本性保証電子保存方法は、暗号鍵などを記憶する内部記憶媒体を用いて大容量記憶媒体に記憶した電子データの原本性を保証する原本性保証電子保存方法において、前記大容量記憶媒体に保存するファイルのリストを示すファイルリストを暗号化した署名情報並びに該大容量記憶媒体の媒体識別情報に基づいて前記大容量記憶媒体の正当性を検証することを特徴とする。

【００１５】この請求項４の発明によれば、大容量記憶媒体に保存するファイルのリストを示すファイルリストを暗号化した署名情報並びに該大容量記憶媒体の媒体識別情報に基づいて大容量記憶媒体の正当性を検証することとしたので、大容量記憶媒体の状態を過去の状態に戻すというような大容量記憶媒体の不正なすり替えを効率良く防止することができる。

【００１６】また、請求項５の発明に係る原本性保証電子保存方法は、前記大容量記憶媒体に保存する保存ファイルのリストを示すファイルリストのハッシュ値を暗号化したリスト署名と、前記大容量記憶媒体の媒体識別情報とを対応づけた媒体認証コードリストを作成する媒体認証コードリスト作成工程と、前記媒体認証コードリスト作成工程により作成された媒体認証コードリストに基づいて前記大容量記憶媒体の正当性を検証する正当性検証工程と、を含んだことを特徴とする。

【００１７】この請求項５の発明によれば、大容量記憶媒体に保存する保存ファイルのリストを示すファイルリストのハッシュ値を暗号化したリスト署名と、大容量記憶媒体の媒体識別情報とを対応づけた媒体認証コードリストを作成し、作成した媒体認証コードリストに基づいて大容量記憶媒体の正当性を検証することとしたので、この媒体認証コードリストを用いて大容量記憶媒体の正当性を効率良く検証することができる。

【００１８】また、請求項６の発明に係る原本性保証電子保存方法は、前記媒体認証コードリスト作成工程により作成された媒体認証コードリストを前記内部記憶媒体に格納し、前記大容量記憶媒体を装置本体に装着する際に、前記内部記憶媒体に格納された媒体認証コードリストに基づいて前記大容量記憶媒体の正当性を検証することを特徴とする。

【００１９】この請求項６の発明によれば、媒体認証コードリストを前記内部記憶媒体に格納し、大容量記憶媒体を装置本体に装着する際に、この内部記憶媒体に格納された媒体認証コードリストに基づいて大容量記憶媒体の正当性を検証することとしたので、内部記憶媒体を有効に利用して大容量記憶媒体の正当性を効率良く検証することができる。

5

【００２０】また、請求項７の発明に係る記録媒体は、前記請求項３～６のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項３～６の動作をコンピュータによって実現することができる。

【００２１】

【発明の実施の形態】以下に添付図面を参照して、この発明に係る原本性保証電子保存方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【００２２】図１は、本実施の形態に係る原本性保証電子保存方法を実行する電子保存装置のブロック構成図である。ユーザは、ホスト計算機２側からネットワーク（単なる通信路で良い）を介して電子保存装置１に対して電子データの保存処理や読み出し処理を実行することができる。

【００２３】図１に示す電子保存装置１において、１１はプロセッサを、１２はネットワークを介して計算機２と通信を行うための通信ポートを、１３は電子データを保存するハードディスクやＣＤ－Ｒ等の大容量記憶媒体を、１４は主制御プログラム，ハッシュプログラム，鍵生成プログラム，暗号化プログラム，復号プログラム等の原本性保証電子保存方法を実現するためのプログラムが格納されたＥＥＰＲＯＭ，ＲＯＭ等で構成されたプログラム格納媒体を、１５は装置プライベートキー，装置公開鍵証明書，最新ファイル識別番号，媒体認証コードリストなどが記憶される内部記憶媒体を、１６はＩＣカード３が挿入されるＩＣカードリーダ／ライタを、１７はタイマをそれぞれ示している。

【００２４】図１に示す大容量記憶媒体１３としては、光磁気ディスクやＣＤ－Ｒのように電子保存装置１から取り外し可能であるが、その他のブロックは電子保存装置１として物理的に一体化されており、通信ポート１２を介する以外に外部からアクセスできないように構成されている。すなわち、図１に示す電子保存装置１は、各ブロックに対して直接アクセスする方法のない耐タンパー性を持った装置である。

【００２５】耐タンパー性を確保するレベルとしては、電子保存装置１の筐体を開けることができないようにシールを貼る程度のものから、筐体を開けられてしまった場合には装置が動作しなくなるようなものまで考えられるが、耐タンパー性を持たせることが可能であればどのようなものであっても良い。

【００２６】図１に示す電子保存装置１は、ユーザから保存要求のあったデータを大容量記憶媒体１３に記録するものである。その際、後にデータの改ざんを検出できるようにするため、保存するデータに対して電子保存装置１自身の暗号鍵によりメッセージ認証子を付加する。

6

【００２７】また、電子保存装置１は、大容量記憶媒体１３に記録されているファイルのリストを作成し、それを大容量記憶媒体１３に記録する処理を行う。このリストに対しても、同様にメッセージ認証子を付加する。

【００２８】また、大容量記録媒体１３の不正なすり替えを検出するために、大容量記憶媒体１３に記録されている保存ファイルリストと、それに付加されたメッセージ認証子を検出することで媒体の認証を行う。また、ファイルの作成日などに不正ができないよう、電子保存装置１に内蔵されているタイマ１７から現在時刻を取得し、ファイルの属性情報として管理する。

【００２９】さらに、電子保存装置１内部で、オリジナルとコピーとを区別することができるように、各ファイルには「仮原本」，「原本」，「謄本」といった属性を付与して管理する。属性の付与されていないファイルは「一般」ファイルと呼ぶことにする。「原本」の属性が付与されて管理されているファイルに対し、外部から複製の作成を要求すると、複製されたファイルには「謄本」という属性が付与される。

【００３０】この属性コードは、他のファイル属性情報と共に、データファイルと関連付けられたファイル属性情報ファイルとして大容量記憶媒体１３に記録され、データファイルと同様、メッセージ認証子を付加して外部から変更することができないように管理される。

【００３１】そして、大容量記憶媒体１３を取り外して外部でその属性が改ざんされたような場合には、そのファイル属性情報ファイルに付与したメッセージ認証子を検証した際にその改ざんを検出する。

【００３２】また、大容量記憶媒体１３の媒体識別番号およびリスト装置署名の対からなる媒体認証コードリストを上記内部記憶媒体１５内に格納し、この媒体認証コードリストを用いた媒体認証をおこなうことにより、大容量記憶媒体１３の状態を過去の状態に戻すというような大容量記憶媒体１３の不正なすり替えを検出する。

【００３３】次に、前述した構成を有する電子保存装置１を用いて実行される原本性保証電子保存方法について、（１）電子データの保存処理、（２）保存ファイルリストの検証処理の順で具体的に説明する。

【００３４】（１）電子データの保存処理

まず最初に、図１に示した電子保存装置１による電子データの保存処理について図２～図４を用いて説明する。図２は、図１に示した電子保存装置１による電子データの保存処理の概念を説明するための説明図であり、図３および図４は、電子保存装置１による電子データの保存処理手順を示すフローチャートである。

【００３５】以下では、図３～図４のフローチャートに示す電子データ保存処理について、図２を参照しつつ具体的に説明するが、ここでは説明の便宜上、電子データを保存する時点で大容量記憶媒体１３は正当であるものとする。

【００３６】電子保存装置１のプロセッサ１１は、通信ポート１２を介して計算機２から電子データの保存要求を受けた場合、大容量記憶媒体１３がマウントされているか否かを判定する（ステップＳ３０１）。ここで、大容量記憶媒体１３がマウントされていないと判定した場合には（ステップＳ３０１否定）、プロセッサ１１は、エラーにより電子データ保存処理を終了する。

【００３７】一方、大容量記憶媒体１３がマウントされていると判定した場合には（ステップＳ３０１肯定）、通信ポート１２を介してユーザ側（計算機２）から、図２に示すデータ２１およびファイル属性コード２２を受け取る（ステップＳ３０２）。

【００３８】そして、プロセッサ１１は、受け取ったファイル属性コード２２が「原本」または「仮原本」であるか否かを判定する（ステップＳ３０３）。ここで、ファイル属性コード２２が「原本」または「仮原本」でないと判定した場合には（ステップＳ３０３否定）、プロセッサ１１は、エラーにより電子データ保存処理を終了する。

【００３９】一方、ファイル属性コード２２が「原本」または「仮原本」であると判定した場合には（ステップＳ３０３肯定）、タイマ１７から現在時刻を取得するとともに（ステップＳ３０４）、内部記憶媒体１５から装置プライベートキー３１、装置公開鍵証明書３２および最新ファイルの識別番号を取得し（ステップＳ３０５）、最新ファイル識別番号をインクリメントして内部記憶媒体１５に記録する（ステップＳ３０６）。

【００４０】そして、電子データに現在時刻、タイマＩＤ、最新ファイル識別番号およびファイル属性コードを追加して図２に示す保存情報２２とし（ステップＳ３０７）、この保存情報２２についてのハッシュ値２３を計算し（ステップＳ３０８）、計算したハッシュ値２３を装置プライベートキーで暗号化して装置署名２４とする（ステップＳ３０９）。

【００４１】このようにして得た装置署名２４および装置公開鍵証明書を保存情報２２に追加して装置署名済み保存情報２５とし（ステップＳ３１０）、この装置署名済み保存情報２５を保存ファイルとして大容量記憶媒体１３に保存する（ステップＳ３１１）。

【００４２】そして、この大容量記憶媒体１３から保存ファイルリスト３０を取得し（ステップＳ３１２）、この保存ファイルリスト３０の正当性を検証する（ステップＳ３１３～Ｓ３１４）。その結果、保存ファイルリスト３０が正当でなければ（ステップＳ３１４否定）、エラー処理をおこない、正当であれば（ステップＳ３１４肯定）、書き込み禁止であるか否かをさらに調べる（ステップＳ３１５）。

【００４３】そして、書き込み禁止であれば（ステップＳ３１５肯定）、エラー処理をおこない、書き込み禁止でなければ（ステップＳ３１５否定）、保存ファイルリスト３０からファイルリストを取得して、先の保存ファイル２６のエントリを追加し（ステップＳ３１６）、ファイルリストについてハッシュ値を計算する（ステップＳ３１７）。

【００４４】そして、このハッシュ値を装置プライベートキーにより暗号化し、リスト装置署名とし（ステップＳ３１８）、このリスト装置署名および装置公開鍵証明書をファイルリストに追加して、新たな保存ファイルリスト３０とし（ステップＳ３１９）、この保存ファイルリスト３０を大容量記憶媒体１３に記録する（ステップＳ３２０）。

【００４５】その後、大容量記憶媒体１３から媒体識別番号を取得し（ステップＳ３２１）、該媒体識別番号とリスト装置署名２９との対を内部記憶媒体１５の媒体認証コードリスト３４に記録する（ステップＳ３２２）。このように、内部記憶媒体１５上に媒体認証コードリスト３４を記録する理由は、この媒体認証コードリスト３４を用いて大容量記憶媒体１３の媒体認証をおこなうためである。

【００４６】上記一連の処理をおこなうことにより、電子データを大容量記憶媒体１３に保存する際に、媒体識別番号およびリスト装置署名２９からなる媒体認証コードリストを内部記憶媒体１５に保存することができる。

【００４７】なお、保存ファイルリスト３０の署名が正しくとも、装着されている大容量記憶媒体１３が所定のフォーマットで初期化されていない場合や、大容量記憶媒体１３内の保存ファイルリスト３０が最新の状態でない場合には、書き込みをおこなうことはできないが、かかる場合であっても大容量記憶媒体１３からの読み出しはできるものとする。

【００４８】（２）保存ファイルリストの検証処理

ところで、上記一連の処理では、大容量記憶媒体１３が正当なものであることを前提としたが、大容量記憶媒体１３の状態を過去の状態に戻すというような大容量記憶媒体１３の不正なすり替えがおこなわれる可能性がある。このため、本実施の形態では、大容量記憶媒体１３を装置本体に装着してマウント処理をおこなう際に、下記に示す保存ファイルリストの検証処理をおこなって、媒体の妥当性を検証する。

【００４９】図５は、図１に示す電子保存装置１がおこなう保存ファイルリストの検証処理手順を示すフローチャートである。同図に示すように、保存ファイルリストの検証処理をおこなう際には、まず最初に大容量記憶媒体１３から保存ファイルリスト３０を取得し（ステップＳ５０１）、該保存ファイルリスト３０のファイルリストに対してハッシュ値を計算し（ステップＳ５０２）、保存ファイルリスト３０の装置公開鍵証明書からパブリックキーを取得する（ステップＳ５０３）。

【００５０】そして、保存ファイルリスト３０のリスト装置署名を取得し（ステップＳ５０４）、取得したリス

ト装置署名をパブリックキーで復号し（ステップＳ５０５）、復号したものがハッシュ値と一致するか否かを調べる（ステップＳ５０６）。

【００５１】そして、両者が一致しない場合には（ステップＳ５０６否定）、エラー処理をおこない、両者が一致する場合には（ステップＳ５０６肯定）、大容量記憶媒体１３から媒体識別番号を取得するとともに（ステップＳ５０７）、内部記憶媒体１５から媒体認証コードリスト３４を取得する（ステップＳ５０８）。

【００５２】そして、この媒体認証コードリスト３４に媒体識別番号と一致するものがあるか否かを調べ（ステップＳ５０９）、一致するものがある場合には（ステップＳ５０９肯定）、媒体認証コードリスト３４内の該当するリスト装置署名と先のリスト装置署名とが一致するか否かを確認する（ステップＳ５１０）。その結果、両リスト署名が一致する場合には（ステップＳ５１０肯定）、保存リストファイルが正当であるものとみなす（ステップＳ５１１）。

【００５３】なお、媒体認証コードリスト３４に媒体識別番号と一致するものがない場合（ステップＳ５０９否定）または両リスト署名が一致しない場合には（ステップＳ５１０否定）、保存リストファイルが正当でないものとみなして書き込み禁止状態を保持して終了する。

【００５４】上記一連の処理をおこなうことにより、大容量記憶媒体１３を装置本体に装着してマウント処理をおこなう際に、保存ファイルリストの検証処理をおこなって、媒体の妥当性を検証することができる。

【００５５】上述してきたように、本実施の形態では、電子データを保存する際に、媒体識別番号とリスト装置署名２９との対からなる媒体認証コードリスト３４を内部記録媒体１５に記憶しておき、大容量記憶媒体１３を装置本体に装着してマウント処理をおこなう際に、保存ファイルリストの検証処理をおこなって、媒体の妥当性を検証するよう構成したので、大容量記憶媒体の状態を過去の状態に戻すというような大容量記憶媒体の不正なすり替えを効率良く防止することができる。

【００５６】ところで、契約書などでは、契約する双方が同一原本をそれぞれ保持することが多いため、上記電子データの保存処理やファイル属性コードの変更処理をおこなう際に、原本データを複数作成することもできる。たとえば、３部の原本を要求された場合には、0000123-01、0000123-02および0000123-03というように末尾に番号を追加したものをそれぞれの「原本」ファイルに付与するよう構成すれば、ファイル識別番号の先頭部のみを確認することにより、同じ電子データであることを確認することができる。

【００５７】

【発明の効果】以上説明したように、請求項１の発明によれば、大容量記憶媒体に保存するファイルのリストを示すファイルリストを暗号化した署名情報並びに該大容量記憶媒体の媒体識別情報に基づいて大容量記憶媒体の正当性を検証するよう構成したので、大容量記憶媒体の状態を過去の状態に戻すというような大容量記憶媒体の不正なすり替えを効率良く防止することができる原本性保証電子保存装置が得られるという効果を奏する。

【００５８】また、請求項２の発明によれば、大容量記憶媒体に保存する保存ファイルのリストを示すファイルリストのハッシュ値を暗号化したリスト署名と、大容量記憶媒体の媒体識別情報とを対応づけた媒体認証コードリストを作成し、作成した媒体認証コードリストに基づいて大容量記憶媒体の正当性を検証するよう構成したので、この媒体認証コードリストを用いて大容量記憶媒体の正当性を効率良く検証することができる原本性保証電子保存装置が得られるという効果を奏する。

【００５９】また、請求項３の発明によれば、媒体認証コードリストを前記内部記憶媒体に格納し、大容量記憶媒体を装置本体に装着する際に、この内部記憶媒体に格納された媒体認証コードリストに基づいて大容量記憶媒体の正当性を検証するよう構成したので、内部記憶媒体を有効に利用して大容量記憶媒体の正当性を効率良く検証することができる原本性保証電子保存装置が得られるという効果を奏する。

【００６０】また、請求項４の発明によれば、大容量記憶媒体に保存するファイルのリストを示すファイルリストを暗号化した署名情報並びに該大容量記憶媒体の媒体識別情報に基づいて大容量記憶媒体の正当性を検証するよう構成したので、大容量記憶媒体の状態を過去の状態に戻すというような大容量記憶媒体の不正なすり替えを効率良く防止することができる原本性保証電子保存方法が得られるという効果を奏する。

【００６１】また、請求項５の発明によれば、大容量記憶媒体に保存する保存ファイルのリストを示すファイルリストのハッシュ値を暗号化したリスト署名と、大容量記憶媒体の媒体識別情報とを対応づけた媒体認証コードリストを作成し、作成した媒体認証コードリストに基づいて大容量記憶媒体の正当性を検証するよう構成したので、この媒体認証コードリストを用いて大容量記憶媒体の正当性を効率良く検証することができる原本性保証電子保存方法が得られるという効果を奏する。

【００６２】また、請求項６の発明によれば、媒体認証コードリストを前記内部記憶媒体に格納し、大容量記憶媒体を装置本体に装着する際に、この内部記憶媒体に格納された媒体認証コードリストに基づいて大容量記憶媒体の正当性を検証するよう構成したので、内部記憶媒体を有効に利用して大容量記憶媒体の正当性を効率良く検証することができる原本性保証電子保存方法が得られるという効果を奏する。

【００６３】また、請求項７の発明に係る記録媒体は、前記請求項３～６のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、

そのプログラムが機械読み取り可能となり、これによって、請求項３～６の動作をコンピュータによって実現することができる。

【図面の簡単な説明】

【図１】この実施の形態に係る原本性保証電子保存方法を実行する電子保存装置のブロック構成図である。

【図２】図１に示した電子保存装置による電子データの保存処理の概念を説明するための説明図である。

【図３】図１に示した電子保存装置による電子データの保存処理手順を示すフローチャートである。

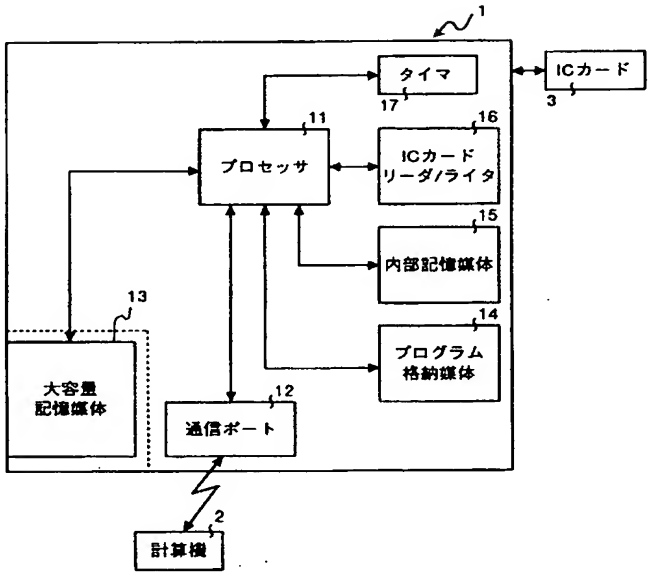
【図４】図１に示した電子保存装置による電子データの保存処理手順を示すフローチャートである。

【図５】図１に示す電子保存装置１がおこなう保存ファイルリストの検証処理手順を示すフローチャートである。

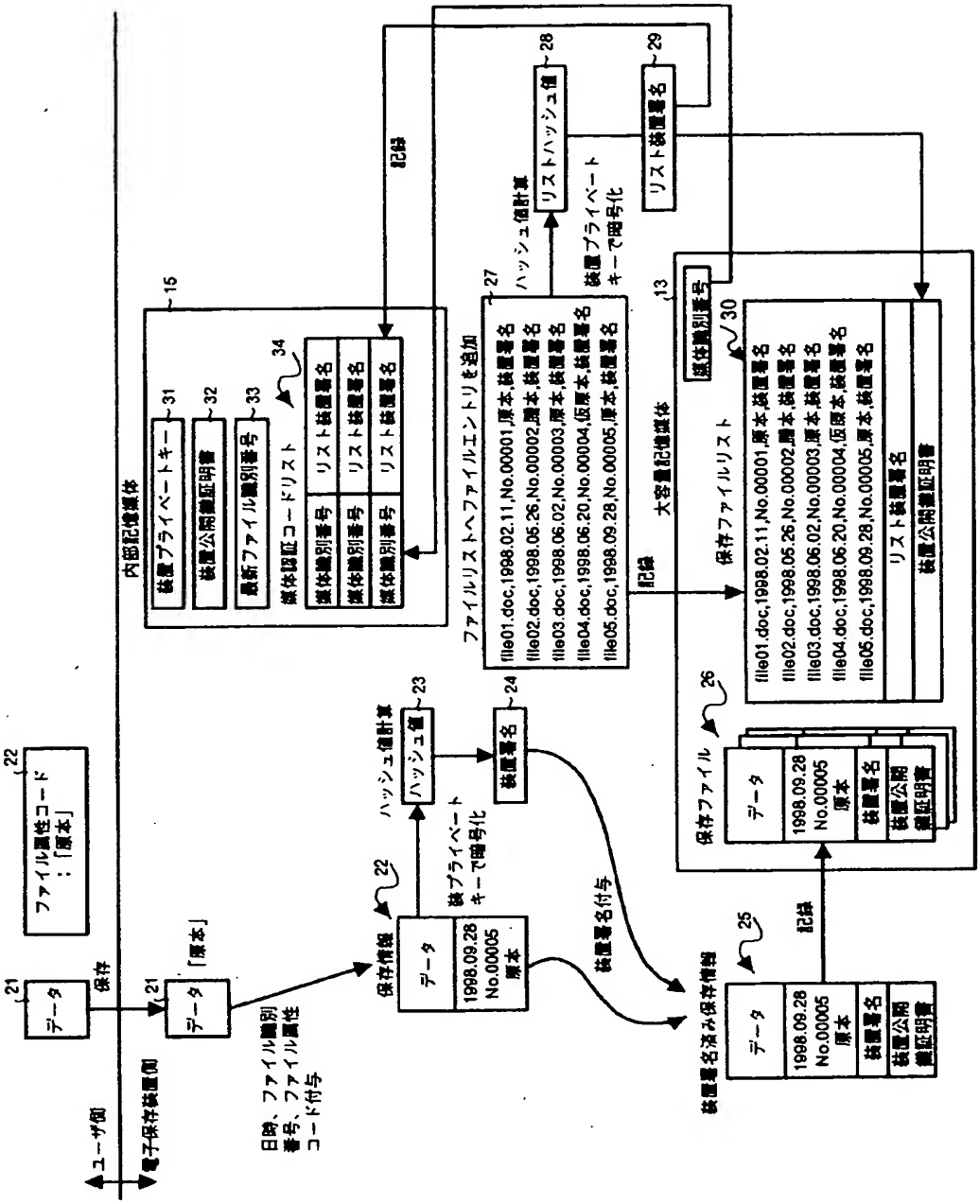
【符号の説明】

１　電子保存装置
２　計算機
３　ＩＣカード
１１　プロセッサ
１２　通信ポート
１３　大容量記憶媒体
１４　プログラム格納媒体
１５　内部記録媒体
１６　ＩＣカードリーダ／ライタ
１７　タイマ
２１　データ
２２　保存情報
２３　ハッシュ値
２４　装置署名
２５　装置署名済み保存情報
２６　保存ファイル
２７　ファイルリスト
２８　リストハッシュ値
２９　リスト装置署名
３０　保存ファイルリスト
３１　装置プライベートキー
３２　装置公開鍵証明書
３３　最新ファイル識別番号
３４　媒体認証コードリスト

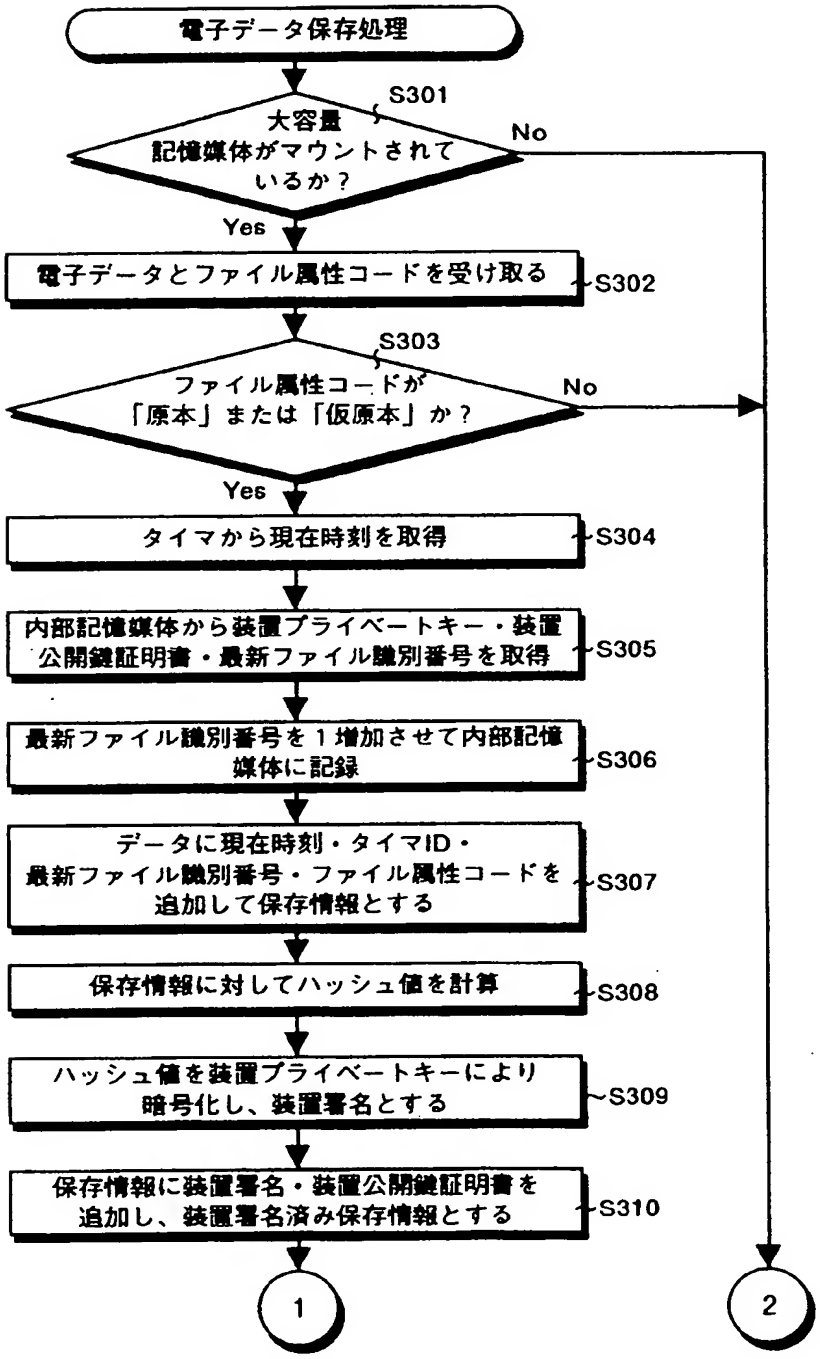
【図１】



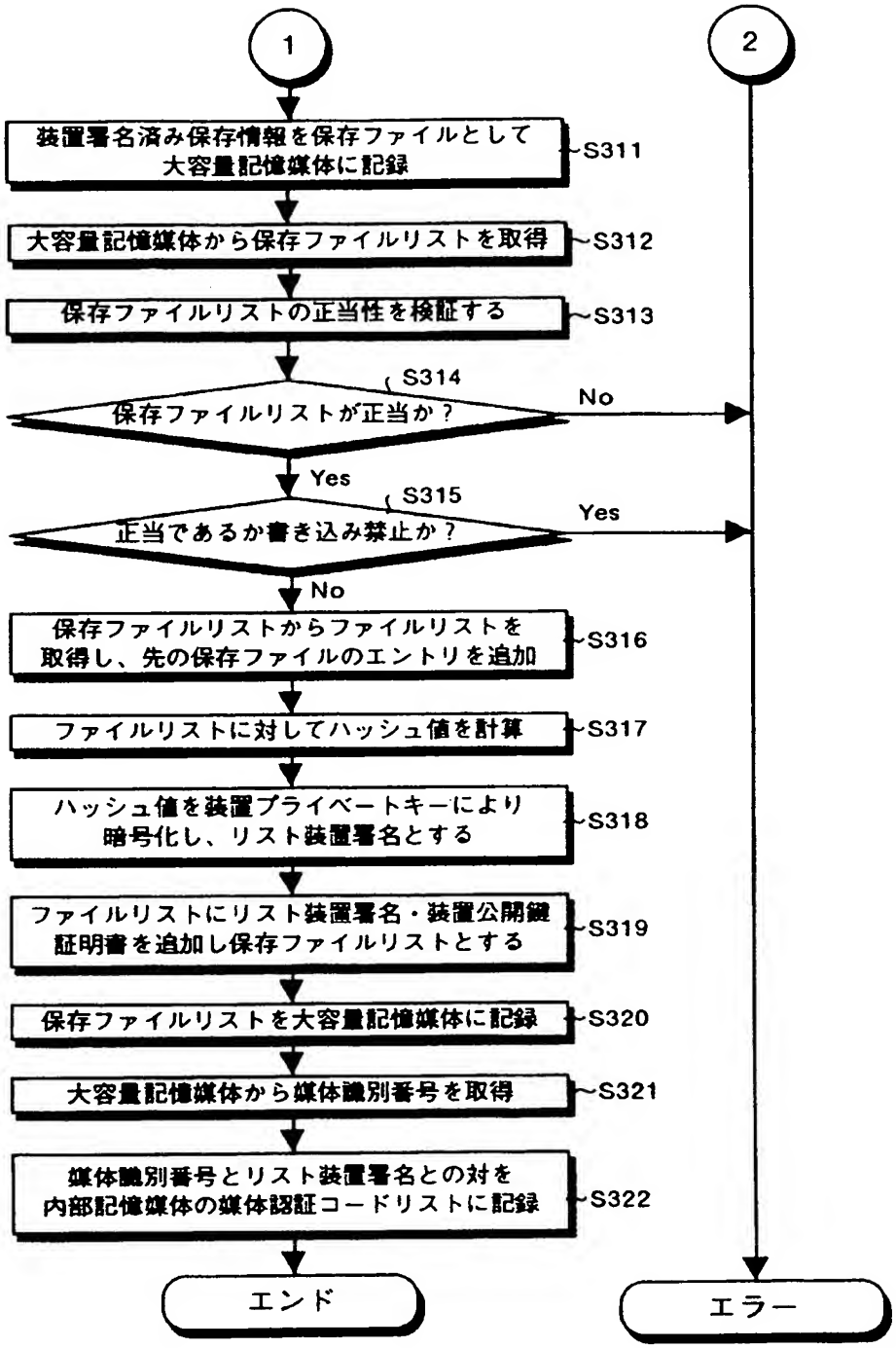
【図２】


ユーザ側
電子保存装置側
保存
データ
ファイル属性コード
：「原本」
「原本」
日時、ファイル識別
番号、ファイル属性
コード付与
保存情報
データ
1998.09.28
No.00005
原本
ハッシュ値計算
ハッシュ値
装置プライベート
キーで暗号化
装置署名
装置署名付与
装置署名済み保存情報
記録
内部記憶媒体
装置プライベートキー
装置公開鍵証明書
最新ファイル識別番号
媒体認証コードリスト
媒体識別番号
リスト装置署名
ファイルリストへファイルエントリを追加
file01.doc,1998.02.11,No.00001,原本,装置署名
file02.doc,1998.05.26,No.00002,原本,装置署名
file03.doc,1998.06.02,No.00003,原本,装置署名
file04.doc,1998.06.20,No.00004,仮原本,装置署名
file05.doc,1998.09.28,No.00005,原本,装置署名
ハッシュ値計算
リストハッシュ値
装置プライベート
キーで暗号化
リスト装置署名
記録
大容量記憶媒体
媒体識別番号
保存ファイルリスト
保存ファイル
リスト装置署名
装置公開鍵証明書

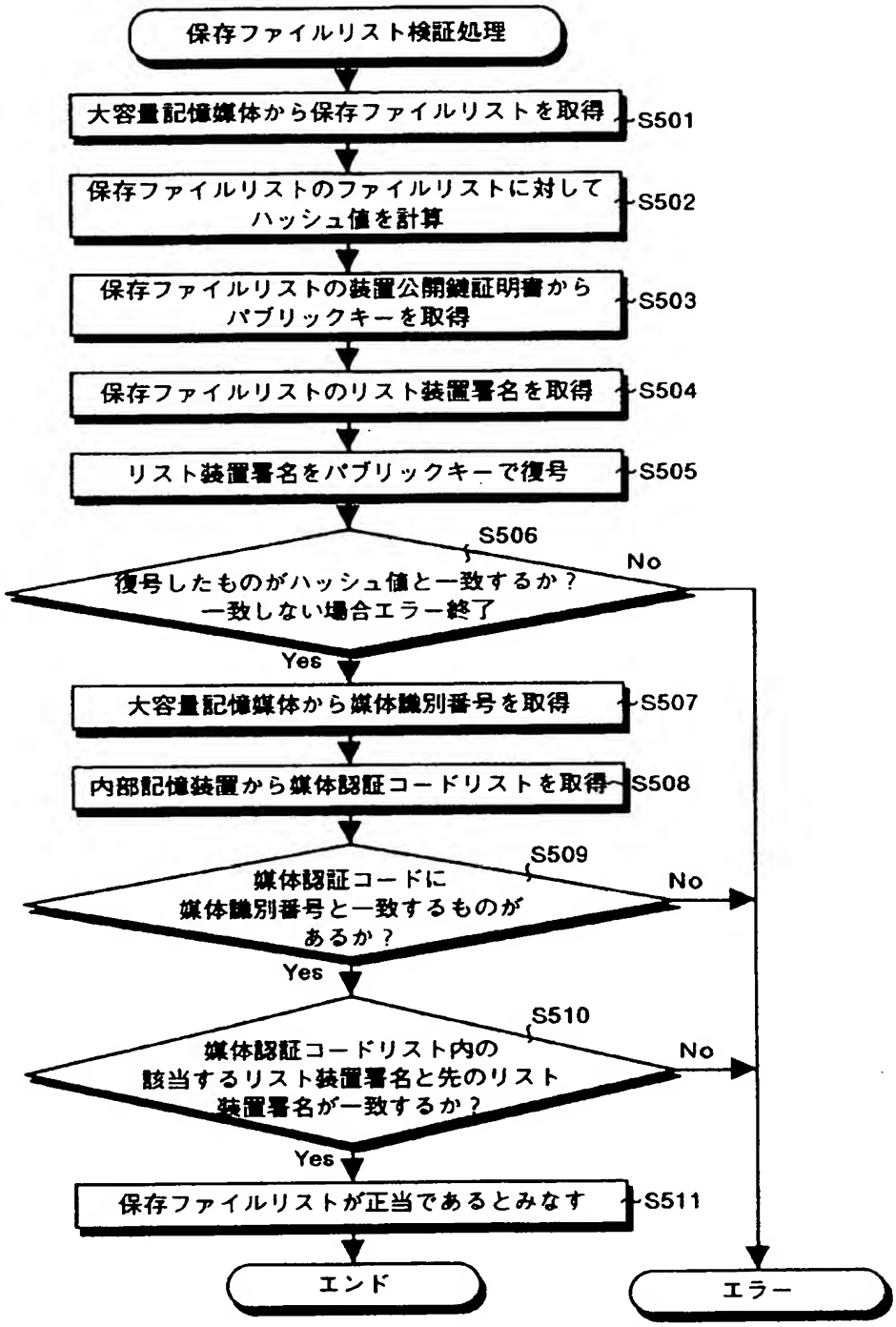
【図３】


電子データ保存処理
S301
大容量記憶媒体がマウントされているか？
No
Yes
電子データとファイル属性コードを受け取る
S302
S303
ファイル属性コードが「原本」または「仮原本」か？
No
Yes
タイマから現在時刻を取得
S304
内部記憶媒体から装置プライベートキー・装置公開鍵証明書・最新ファイル識別番号を取得
S305
最新ファイル識別番号を１増加させて内部記憶媒体に記録
S306
データに現在時刻・タイマID・最新ファイル識別番号・ファイル属性コードを追加して保存情報とする
S307
保存情報に対してハッシュ値を計算
S308
ハッシュ値を装置プライベートキーにより暗号化し、装置署名とする
S309
保存情報に装置署名・装置公開鍵証明書を追加し、装置署名済み保存情報とする
S310
1
2

【図４】


1
2
装置署名済み保存情報を保存ファイルとして大容量記憶媒体に記録
S311
大容量記憶媒体から保存ファイルリストを取得
S312
保存ファイルリストの正当性を検証する
S313
S314
保存ファイルリストが正当か？
No
Yes
S315
正当であるか書き込み禁止か？
Yes
No
保存ファイルリストからファイルリストを取得し、先の保存ファイルのエントリを追加
S316
ファイルリストに対してハッシュ値を計算
S317
ハッシュ値を装置プライベートキーにより暗号化し、リスト装置署名とする
S318
ファイルリストにリスト装置署名・装置公開鍵証明書を追加し保存ファイルリストとする
S319
保存ファイルリストを大容量記憶媒体に記録
S320
大容量記憶媒体から媒体識別番号を取得
S321
媒体識別番号とリスト装置署名との対を内部記憶媒体の媒体認証コードリストに記録
S322
エンド
エラー

【図５】


保存ファイルリスト検証処理
大容量記憶媒体から保存ファイルリストを取得
S501
保存ファイルリストのファイルリストに対して
ハッシュ値を計算
S502
保存ファイルリストの装置公開鍵証明書から
パブリックキーを取得
S503
保存ファイルリストのリスト装置署名を取得
S504
リスト装置署名をパブリックキーで復号
S505
S506
復号したものがハッシュ値と一致するか？
一致しない場合エラー終了
No
Yes
大容量記憶媒体から媒体識別番号を取得
S507
内部記憶装置から媒体認証コードリストを取得
S508
S509
媒体認証コードに
媒体識別番号と一致するものが
あるか？
No
Yes
S510
媒体認証コードリスト内の
該当するリスト装置署名と先のリスト
装置署名が一致するか？
No
Yes
保存ファイルリストが正当であるとみなす
S511
エンド
エラー

フロントページの続き

Ｆターム(参考) 5B065 CC08 PA04 PA14 PA16 ZA04
ZA15
5J104 AA09 LA03 LA06 NA12 NA27
PA07 PA14
9A001 DD09 EE03 JJ07 LL03